СОФИЙСКИ УНИВЕРСИТЕТ
„СВ. КЛИМЕНТ ОХРИДСКИ"

SOFIA UNIVERSITY
ST. KLIMENT OHRIDSKI

Курсова работа

по

Социално-правни аспекти
на софтуерното инженерство

на тема

„Престъпления, свързани с
информационните технологии"

Автор: Стефка Москова
Факултет: ФМИ
Специалност: Софтуерно инженерство
Курс: III
Факултетен №: 61979

Съдържание

Нека само си зададем въпроса щеше ли да видим чудото, наречено Интернет, във вида, в който го познаваме днес, без наличието на компютърните измами. А нека дори за миг си представим съвременния свят, в който Интернет е просто средство за изпращане на документи между големи организации, а не част от нашето ежедневие. Да, обществото ни със сигурност се промени след популяризирането на Интернет…

I. Наказателен кодекс

Терминът ***„наказателно право“*** пряко се отнася до действителните закони, устави и правила, които определят деянията и поведението в престъпленията. Наказателното право установява наказанията за всеки вид престъпление. Престъпните действия/криминалните прояви обикновено са тези, които правителството разглежда, за да не се стига до нарушение на общественото благосъстояние или безопасност. Самата дефиниция за наказателно право:

*„**Наказателно право** - областта на местното, държавното и федералното законодателство, която дефинира престъпни деяния, урежда арестуването, задържането, обвиняването и наказателното преследване на обвиняемите извършители и определя конкретни наказания.“*

подсказва, че ***наказателното право*** е кодифицирано в ***Наказателен кодекс***. То има за цел да защитава човешката личност от престъпни посегателства. ***Наказателният кодекс*** определя кои обществено опасни деяния са престъпления и какви наказания се налагат за тях.

Длъжностните престъпления се делят на същински и несъщински киберпрестъпления. Същински са тези, при които субект на основния състав е длъжностно лице. Несъщински са тези, при които субект на основния състав е всяко наказателно отговорно лице, а когато са извършени от длъжностно лице е предвиден квалифициран случай.

II. Същински киберпрестъпления

„Същински киберпрестъпления са престъпления, при които обект на посегателството са самите технологии – компютърни програми, компютърни данни или функционирането на информационните системи и мрежи.“

1. Активно и неактивно хакерство

Светът се превръща в една голяма връзка с ***WWW (World Wide Web)*** и компютърни системи, като по този начин се излага на голяма заплаха от злонамерени хакери. ***Терминът „хакер“*** обикновено се използва за описване на човек, който навлиза в компютърна система, като заобикаля сигурността и навлиза в неразрешени области на информация.
Хакерството е въображаемо престъпление, което се извършва, когато хакерите пробият в друга отдалечена система с намерението за кражба или манипулиране на информация. Първоначално хакването започва като непланирано явление -

компютърните техници се опитвали да разберат как работят компютърните системи.

В миналото и до днес, се наблюдават много прояви на неактивно хакерство. Някои от тях са световно известни, но за други не се говори. Ето и няколко примера за не толкова прочутите случаи на неактивно хакерство:

- ***Групата на анонимните (Anonymous)***

  Анонимните е името на неформална група хакери. Това е „интернет група“ с много свободна и децентрализирана структура на властта, действаща по-скоро според идеи, отколкото според директиви. Анонимните стават известни след серия широко отразени от медиите хакерски атаки срещу правителствени, религиозни и обществени уебсайтове. Участието в движението не е регламентирано, всяка атака може да бъде извършвана от различни хора, които светът не познава и не може да разобличи.

Фиг.1. Маските, с които се отличават Anonymous

- ***Червените хакери (RedHack) – RedHack***

  Червените хакери атакуват сайтовете на държавата, армията, разузнавателните служби и Съвета за научни и технически изследвания на Турция.

Фиг.2. Отличителните белези на RedHack

- ***Групата на Лазарус (Lazarus Group)***

  Lazarus Group (известна още като HIDDEN COBRA) е група за киберпрестъпления, съставена от неизвестен брой лица. Най-известната атака, за която е отговорна групата, е "Операция Троя". Това е кибер-шпионска кампания, която използва непрофесионални техники за DDoS атаки, насочени към южнокорейското правителство в Сеул.

2. Вируси, троянски коне и компютърни измами

Терминът „вирус“ често се използва като общо позоваване на всеки злонамерен код. В тази точка ще разгледаме по-обстойно вирусите, троянските коне и компютърните измами.

Компютърният вирус е малка програма. Тя е написана, за да промени начина на работа на компютъра, без разрешението или познанията на даден потребител. Вирусът трябва да се изпълни сам. Той възпоризвежда свой собствен код в пътя на изпълнение на друга програма. Трябва да се възпроизведе. Например, той може да замени други изпълними файлове с копия на заразения с вирус файл.

Някои вируси са програмирани да повредят компютъра - повреждат програми, изтриват файлове или преформатират твърдия диск. Други не са проектирани да правят никакви щети, а просто да се репликират и да направят присъствието си известно чрез представяне на текстови, видео и аудио съобщения. Дори тези доброкачествени вируси могат да създадат проблеми за потребителя на компютъра. Те обикновено заемат компютърна памет, използвана от законни програми. В резултат на това те често причиняват непостоянно поведение и могат да доведат до сривове в системата. В допълнение, много вируси са подложени на грешки и тези грешки могат да доведат до сривове в системата и загуба на данни.

Троянските коне са ***файлове-измамници***, които твърдят, че са нещо желателно, но всъщност са злонамерени. Много важно разграничение от истинските вируси е, че те не се възпроизвеждат, както вирусите. Троянските програми съдържат злонамерен код, който при задействане предизвиква загуба или дори кражба на данни. За да се разпространи троянски кон, всъщност трябва да поканите тези програми на компютрите си - например, като отворите прикачен файл в имейл.

3. Разпространение на пароли

Няма начин да предотвратим разпространението на паролите. Единственото, което можем да направим от наша страна за личната ни парола, е да следваме стъпки или съвети, с които да направим паролата си трудна за отгатване и разпространение. В началото, когато започвах да навлизам в информационните технологии, учителката ми по информатика казваше: „Направете си парола, която не е смислено изречение, отключете фантазията си!“. Започнах се да се замислям как да си измисля трудна парола и в същото време тя да е лесно запомняща се. А защо не – от едно смислено изрезение, по избор, да взема само първите букви от думите. Така и се получи. Например: ***“The quick brown fox jumped over the lazy dog”*** може да се преобразува в парола – ***Tqbfjotld***. Трудна за разбиране и лесна за запомняне, нали?

III. Несъщински киберпрестъпления

Несъщинските киберпрестъпления представляват унищожаване или повреждане на чужда вещ чрез манипулиране на информация, заради което законът предвижда по-тежко наказание. Например:

1.Нарушение на авторски права

Авторското право е това, което предпазва оригиналните произведения от това да бъдат неправилно дублирани и разпространени. Пример за нарушаване на авторските права е незаконното изтегляне и споделяне на музика, филми и други защитени авторски права. Има закони за защита на хората, чиито материали са защитени с авторски права. Асоциацията на звукозаписната индустрия на Америка, например, е група, която се опитва да премахне онези, които незаконно изтеглят и споделят музика чрез използването на техните компютри. През изминалата година те са подали много съдебни дела и ще продължат да го правят, за да защитят собствениците на авторски права, като артисти и звукозаписни компании. Друг пример е университетът в Минесота, Крокстън, който също се опитва да попречи на учениците да извършват незаконния акт за изтегляне и споделяне на файлове на компютрите си. Ще продължат да се предприемат действия от страна на училището и закона, докато този проблем не бъде напълно уреден.

2.Детска порнография

Интернет е метод за комуникация и източник на информация, която става популярна сред онези, които се интересуват от информационната “супермагистрала”.
Проблемът с този свят, който познаваме като киберпространство или мрежата, е, че част от тази информация, включително порнографски материали и нецензурирана информация, е достъпна за непълнолетни. Знаете ли, че 83.5% от изображенията в интернет са порнографски? Знаете ли, че интернет порнографията и нецензурираната информация са достъпни за любопитни деца, които се натъкват на тях? А знаете ли, че 45.3% от тези порнографски изображения са на деца?

3.Тайна на е-кореспонденцията

В днешно време може би вече няма човек, който да не е комуникирал или водил кореспонденция по електронен път. Дали по професионален ангажимент чрез строго секретна мрежа, дали по имейл, дали просто чат в някое мобилно приложение като Messenger, WhatsApp, Viber, Line или пък приложения за запознанства – Tinder/Badoo. Много е хубаво човек да комуникира лесно със събеседниците си, независимо от средата за провеждане на разговорите, но никой не се замисля, дали кореспонденцията се следи, дали събеседникът е сигурен и сериозен човек, на който може да се довери. Чувала съм за много случаи с посегателство върху лични данни и злоупотреба със споделени снимки в мобилни приложения. Човек винаги трябва да има едно наум и винаги да бъде внимателен на кого, как и колко се доверява.





IV. Синтаксис и семантика на документа

Синтаксис на документа:

- Всички нови думи, важни термини и дефиниции са **удебелени** и ***наклонени***.
- Цитирането е обозначено с „“.
- Важните точки от документа са **удебелени** и **уголемени**.

Семантика на документа:

- Документът включва заглавна страница;
- Документът включва съдържание;
- Документът включва 5 основни точки:
    - Наказателен кодекс – включва дефиниция и лично виждане за криминалните прояви;
    - Същински киберпрестъпления – обект на посегателство е самата технология;
    - Несъщински киберпрестъпления – престъплението се извършва посредством технологии, тоест като средство;
    - Синтаксис и семантика на документа – описание на навигацията по документа;
    - Използвана литература – използвани литературни източници за идеи по съставянето на курсовата работа;

V. Използвана литература

1. T. Nagel, 1979, Mortal Questions;
2. J. Raz, 1986, The Morality of Freedom;
3. M. Redmayne, 2015, Bad Character in the Criminal Trial;
4. P. Roberts, 2005, Strict Liability and the Presumption of Innocence: An Expose of Functionalist Assumptions;
5. L. Alexander, 2002, Criminal Liability for Omissions – An Inventory of Issues;
6. L. Alexander, 2009, Crime and Culpability: A Theory of Criminal Law;
7. A. Ashworth, 1993, Taking the Consequences;
8. M. Thorburn, 2011, Constitutionalism and the Limits of the Criminal Law;
9. S. Green, 2011, Criminal Law as Public Law;
10. H. Stewart, 2014, “The Right to Be Presumed Innocent”

„Когато се появи интернет, се оказа, че съществува свят без стени и врати. Вместо тях има връзка. Ти не знаеш, къде ще те заведе, но ясно осъзнаваш, че това е връзка със света. Мен не ме изненадва, че хората влизат във виртуалното пространство.“

Рутгер Хауер